第一章 计算机网络与互联网络

1.1 什么是互联网络

- 从构成角度看
  - 点：端系统（如PC、手机、服务器等），分组交换设备（如路由器、交换机等）
  - 边：链路
  - 互联网络 是网络的网络

- 从服务的角度来看：互联网络—能够为应用提供通信服务的通信架构（有连接可靠的服务和无连接不可靠的服务）—使用通信服务相互配合工作的应用

- 协议：对等层实体在通信过程中所遵循的规则的集合
  - 语法+语义+时序
  - 协议定义了在两个或多个通信实体之间交换的报文格式和次序，以及在报文传输和/或接收或其他事件方面所采取的动作

应用层协议	HTTP	FTP	SMTP	POP3	IMAP	DNS	DHCP
传输层协议	TCP					UDP	
网络层协议	IP	ICMP	IPX*、DECnet*			RIP	
数据链路层协议	PPP HDLC	TDMA FDMA CDMA	ALOHA Slotted ALOHA CSMA CSMA/CD	Polling	Taken-passing	ARP	
物理层协议							

1 B = 8 b （即1Byte（字节） = 8bits（位/比特位））
bps = b/s
G M K m u n
10的12次方 |太[拉] | T
10的 9次方 |吉[咖] | G
10的 6次方 | 兆 | M
10的 3次方 | 千 | k
10的 2次方 | 百 | h
10的 1次方 | 十 | da

10的-1次方 | 分 | d
10的-2次方 | 厘 | c
10的-3次方 | 毫 | m
10的-6次方 | 微 | μ
10的-9次方 |纳[诺] | n
10的-12次方 |皮[可] | p

第一章 计算机网络与互联网络

1.2 网络边缘　1.3 网络核心

- 网络的结构—网络边缘（应用，主机）+网络核心（路由器）+接入网络与通信链路
- 网络边缘：也叫资源子网，实现资源共享，主要有主机、服务器这些端系统。运行全部5层协议

  按照端系统中的应用交互方式划分：　理解
  - C/S模式，特点
  - P2P模式，特点
- 利用网络的服务：
  - 面向连接的服务
  - 无连接的服务
- 网络核心：也叫通信子网，实现数据交换、网络通信功能
  - 组成：网络交换设备 如：路由器、交换、通信链路
  - 功能：数据交换
- 数据交换方式
  - 分组交换：存储转发方式， 统计复用　好处、代价
  - 线路/电路交换：FDM、TDM、WDM　缺陷

网络边缘和网络核心是网络中重要的两部分（子网）！
网络核心和网络边缘的作用、主要设备要能说清！

第一章 计算机网络与互联网络

1.4 接入网

- 将端系统连接到边缘路由器的链路或网络
- 住宅/家庭接入：点到点接入
  - ADSL：利用电话网
  - HFC: hybrid fiber coax, 利用有线电视网，Cable Modem 是其特殊的调制解调器
  - FTTH: 光纤到户
- 机构接入：LAN
  - 以太网络
  - WLAN
- 无线广域接入

- 物理链路
  - 导引型介质
  - 非导引型介质
- 常用介质 理解
  - TP双绞线：由两根绝缘铜线绞合而成，能减少邻近类似的双绞线的电气干扰。
  - 同轴电缆：由两个同心铜导体组成
  - 光纤：不受电磁干扰，衰减极低，很难窃听
  - Radio

了解常用的网络传输介质及其特点

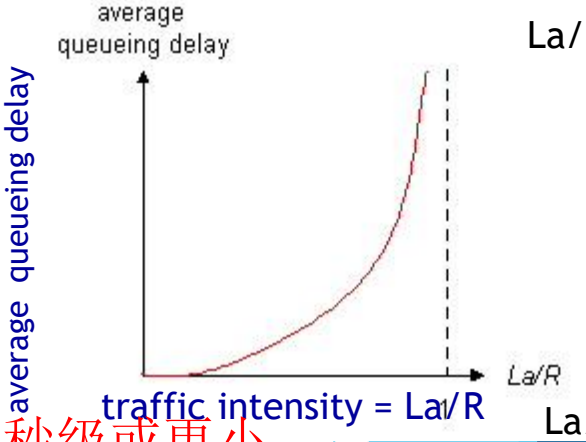
第一章 计算机网络与互联网络

1.5 Internet结构和ISP

- 近似层次型结构
  - T-1 ISP
  - T-2 ISP（Regional ISP）
  - Local ISP
- ISP之间的连接
  - 对等连接
  - IXP
  - POP: point-of-presence，上层ISP通告POP接入下层ISP）
- 内容提供商网络（ICP）
  - 内容提供商Data center自己之间的访问，通过自己部署的专网
  - 用户接入后通过离用户最近的DC为之服务
- 这种组织方式是一个松散的层次结构，各个ISP之间的网络互联是任意的。

第一章 计算机网络与互联网络

1.6 分组延时、丢失和吞吐量



- 4类延迟
  - 处理延迟——设备本身能力，通常是微秒级或更小
  - 排队延迟——流量强度概念、计算公式 L×a/R
  - 传输延迟（发送延迟）——带宽R和分组长度L，L/R
  - 传播延迟——电磁波/光速s和链路长度d，d/s
- 丢失原因：缓冲区溢出、出错没通过校验、TTL=0——重传
- 吞吐量
  - 瞬间吞吐量
  - 平均吞吐量
  - 瓶颈链路决定了主机之间的吞吐量（从每段链路获得的大致带宽是1/N，瓶颈链路是所有链路段中获得带宽最小的）
- 掌握计算机网络的性能指标：吞吐量、带宽、时延、速率、时延带宽积、往返时间、利用率

第一章 计算机网络与互联网络

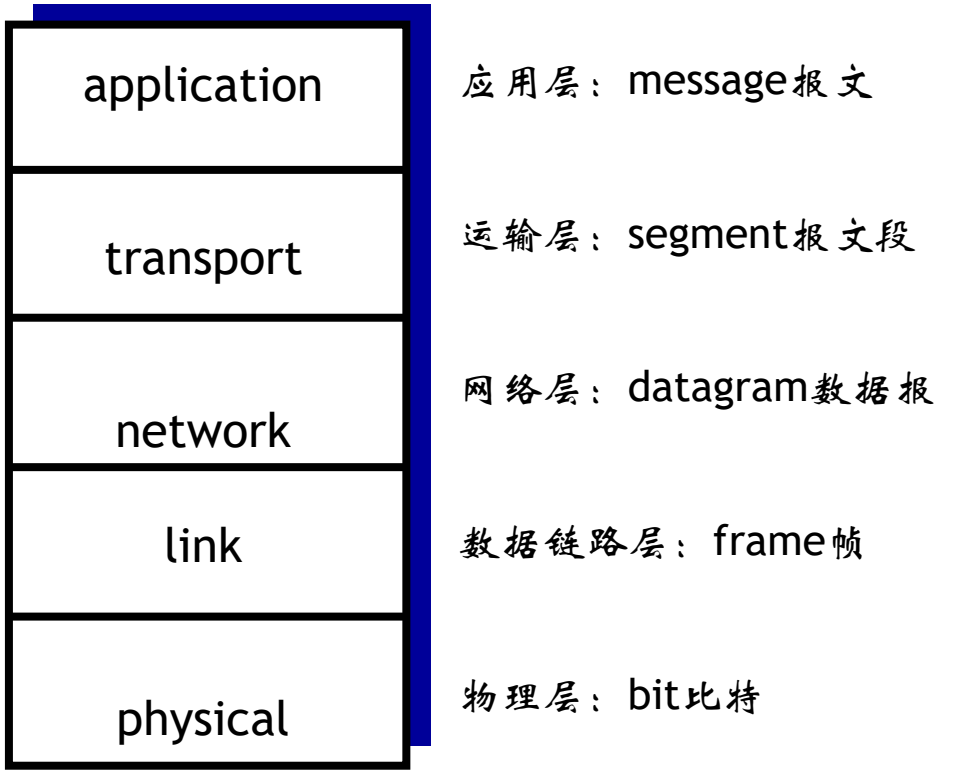
1.7 协议层次及服务模型

- 分层
  - 将复杂的网络功能划分成功能明确的层次，上层利用下层提供的服务来实现本层的协议，从而为上层提供更复杂的功能
- 术语和概念
  - 服务、服务访问原语，服务访问点
  - 面向连接的服务，无连接的服务
  - 协议，协议是对等层的实体再交互的过程中遵守的规则的集合
  - 协议数据单元PDU
  - 服务和协议之间的关系（区别与联系）本层协议的实现要靠下层提供的服务来实现；本层实体通过协议为上层提供更高级的服务
- 互联网络分层模型及每一层的功能
  - OSI/RM建议模型
  - TCP/IP分层模型
- 封装和解封装

1.8 安全及历史

第一章 计算机网络与互联网络

1.7 协议层次及服务模型



- TCP/IP分层模型

- OSI/RM建议模型

Internet分层	各层的分组（packet）名称	
应用层 Application layer	message：报文	主机（端系统）
运输层 Transport layer	segment：报文段	端口port 主机（host）
网络层 Network layer:	datagram：数据报	IP地址 路由器（router）
链路层 Link layer	frame：帧	MAC地址 交换机（switch）
物理层 Physical layer	bit (bit flow): 比特(比特流)	

第二章 应用层

2.1 网络应用原理

- 应用架构
  - C/S客户端-服务器模式　掌握其工作原理
  - P2P模式
  - 混合模式
- 进程间通信
  - 同主机：操作系统定义的通信方法
  - 不同主机：利用网络提供的架构（TCP/IP）交换报文
  - 应用层服务和功能：实现不同主机之间进程与进程之间的通信
- 套接字（Socket）
  - 分布式应用进程之间的门，传输层协议提供的端到端服务接口；操作系统用于标示应用通信关系所采用的本地标示
  - TCP：连接的本地标示
  - UDP：端节点的本地标示
- 进程编址：IP+PORT（本质上在传输层上应用了端口号，用于区分应用，TCP和UDP使用端口号的方式不同）

第二章 应用层 2.1 网络应用原理

- 网络所提供服务的主要指标
  - 数据完整性
  - 定时/延迟
  - 吞吐量
  - 安全
- TCP服务：面向连接、可靠数据传输（字节流）、流量控制、拥塞控制
- UDP服务：无连接，不可靠的服务

（多选）UDP不能提供的运输服务有哪些?

A、可靠数据传输 B、吞吐量 C、定时 D、安全性

（多选）TCP和UDP都不能保证能提供的服务有哪些?

A、可靠数据传输 B、吞吐量 C、定时 D、安全性

Socket（套接字）

- 如果Socket API每次传输报文，都携带如此多的信息，太繁琐易错，不便于管理
- 用个代号标示通信的双方或者单方：socket
- 就像OS打开文件返回的句柄一样
  - 对句柄的操作，就是对文件的操作

- **应用编程接口 API 称为 socket API，简称为 socket。**
- **socket API 中使用的一个函数名也叫作 socket。**
- **调用 socket 函数的端点称为 socket。**
- **调用 socket 函数时其返回值称为 socket 描述符，可简称为 socket。**
- **在操作系统内核中连网协议的 Berkeley 实现，称为 socket 实现。**

第二章 应用层 2.2 web 和 HTTP

- Web应用
  - HTTP协议、HTML、客户端、服务器
  - 网页、对象、URL（网页中包含多个对象，每个对象有一个唯一的URL对其定位）、通用80号端口
  - URL格式：Prot://user:psw@www.someschool.edu/someDept/pic.gif:port
    协议名 用户:口令 host name path name port
- HTTP协议
  - 定义了客户端服务器之间通信的报文格式、解释和时序
  - 持续型HTTP、非持续型HTTP
  - HTTP工作流程：客户端请求建立TCP连接－服务器响应TCP连接－客户端发送HTTP请求报文－服务器返回HTTP响应－释放TCP连接。
  - HTTP是无状态协议：服务器不维护关于客户的任何信息
  - 报文格式：请求报文、响应报文

GET：请求，POST：上载，HEAD：获得头部信息
HOST：请求的主机名，允许多个域名同处一个IP地址，即虚拟主机
User-Agent：产生请求的浏览器类型。
Accept：客户端可识别的内容类型列表。
Connection：close表示非持续连接，keep-alive表示持续连接

状态行(协议版本、状态码及描述)

header lines

```
HTTP/1.1 200 OK\r\n
Date: Sun, 26 Sep 2010 20:09:20 GMT\r\n
Server: Apache/2.0.52 (CentOS)\r\n
Last-Modified: Tue, 30 Oct 2007 17:00:02
   GMT\r\n
ETag: "17dc6-a5c-bf716880"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 2652\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-
   1\r\n
\r\n
data data data data data ...
```

data, e.g., requested HTML file

Date：该报文生成日期，
Server：服务器类型
Last-Modified：报文数据上一次修改时间。
Content-Length：报文携带的数据长度。
Connection：close表示非持续连接，keep-alive表示持续连接
Content-Type：数据类型

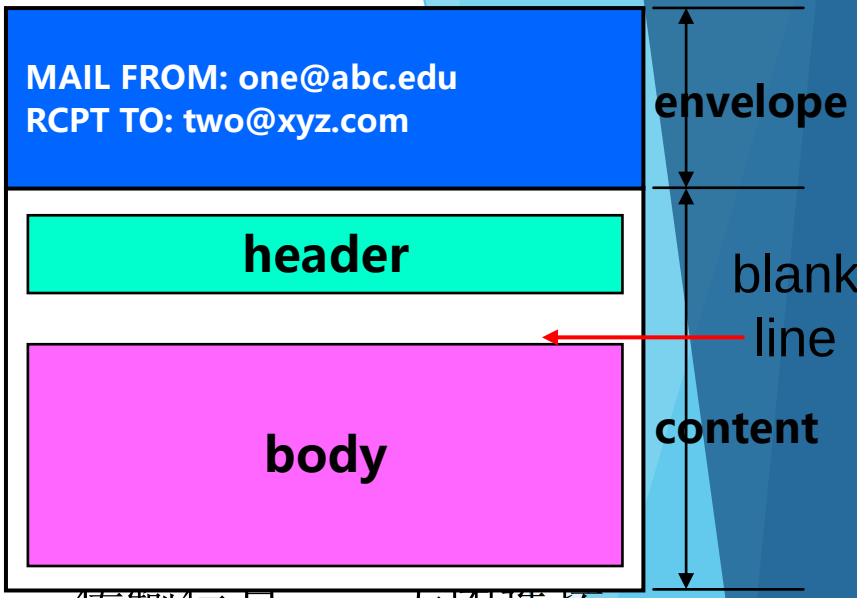
第二章 应用层 2.2 web 和 HTTP

- 响应报文状态码
  - 200 OK
  - 301 Moved Permanently 重定向，客户端软件自动用新的URL去获取对象（重定向）
  - 400 Bad Request
  - 404 Not Found
  - 505 HTTP Version Not Supported
- COOKIES
  - 将HTTP协议从无状态改造为有状态协议
- WEB缓存
  - 作用：通过本地 命中，减少这些对象的访问延迟，进一步减少接入链路的流量强度，从而降低排队延迟带来总体平均延迟的减少，减轻服务器负担。

第二章 应用层 2.3 FTP

- 构成
  - FTP协议、客户端、服务器
  - FTP常见命令和状态码
- FTP工作流程
  - TCP应用
  - FTP 服务器使用21号端口，等待客户端访问
  - 客户端使用自身端口号请求建立TCP连接，客户端通过验证控制连接建立
  - 客户端浏览远程文件夹，通过控制连接向服务器发送请求命令
  - 服务器收到数据传输命令，通过20号端口主动向客户端建立TCP连接（数据连接），传输数据
  - 传输数据完成后，服务器关闭数据连接。
  - 控制连接（带外连接）使用21号端口，数据连接（带内连接）使用20号端口

第二章 应用层



2.4 EMAIL

- 构成
  - 用户代理、邮件服务器、SMTP
- SMTP协议
  - 使用TCP25号端口
  - 工作流程：建立连接——握手——传输信息——关闭连接
  - 与HTTP对比：HTTP：拉；SMTP：推
  - 邮件格式：报文头、报文体
  - MIME：邮件多媒体扩展，可以在邮件中编解码多媒体应用
- 邮件存取协议
  - 常用：IMAP、POP3
  - IMAP使用TCP143号端口，POP3使用TCP110号端口

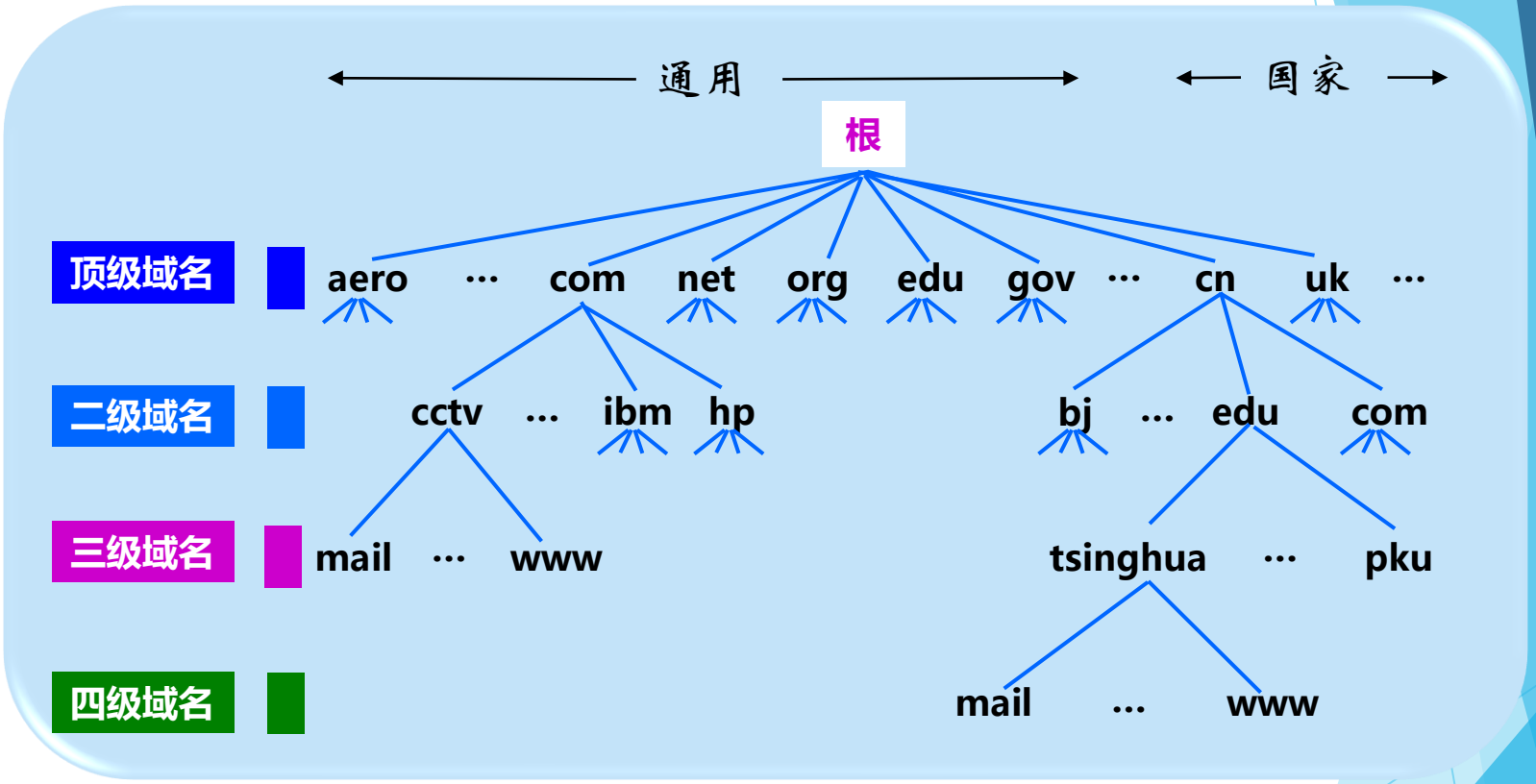
（多选）目前流行的邮件访问协议有哪些?

A、POP3 B、IMAP C、HTTP D、FTP

第二章 应用层

2.5 DNS

- 作用
  - 完整域名到IP地址的转换；别名到规范名字的转换；邮件服务器名字到规范名字的转换；负载均衡
  - DNS是应用层面的互联网基础设施，是供其他应用使用的应用
  - UDP应用，使用53号
- 域名 层次结构
  - …. 三级域名 . 二级域名 . 顶级域名
  - 顶级域名：通用（如.com；.edu；.gov； .int； .mil； .net； .org；.firm；.web；.arts；.rec)\国家（如.cn ; .us ; .nl ; .jp）和基础结构域名 arpa（用于反向域名解析）
  - 域名信息存储和服务是分布的，每个权威域名服务器担任一个ZONE的名字到IP地址的权威转换，也缓冲名字—IP信息的转换。


通用
国家
根
顶级域名
二级域名
三级域名
四级域名
aero
com
net
org
edu
gov
cn
uk
cctv
ibm
hp
bj
edu
com
mail
www
tsinghua
pku
mail
www

第二章 应用层 2.5 DNS

- 协议
  - 报文：请求和响应格式相同
  - RR：资源记录 RR format: **(name, ttl, class, type, value)**
- 域名解析过程（本地解析器—本地DNS服务器—上层域名服务器—…—权威名字服务器—返回）
  - 递归查询
  - 迭代查询
- DNS缓存

2.6 P2P

- 每个对等体（peer）既是客户端又是服务器
  - P2P网络是这些peer构成的应用层面的逻辑网络
  - P2P内容分发比C/S快：peer节点能够参与到内容的上载，流量和服务是分布的，可扩展性更好。
- BitTorrent

第三章 运输层

3.1 运输层服务

- 能够使分布式端系统应用之间进行逻辑通信
- 运输层服务和网络层服务区别
  - 网络层服务：主机到主机的通信
  - 运输层服务：进程到进程的通信
- 协议
  - 运行于端系统的两个对等运输层实体相互通信应遵守的规则集合
  - TCP：有连接，可靠保序数据传输服务
  - UDP：无连接，不可靠，不保序的数据传输服务

3.2 多路复用和多路分解

- 复用：处理来自多个Socket的数据，添加头部信息
- 解复用：根据头部信息将收到的segment传递到正确的Socket

第三章 运输层

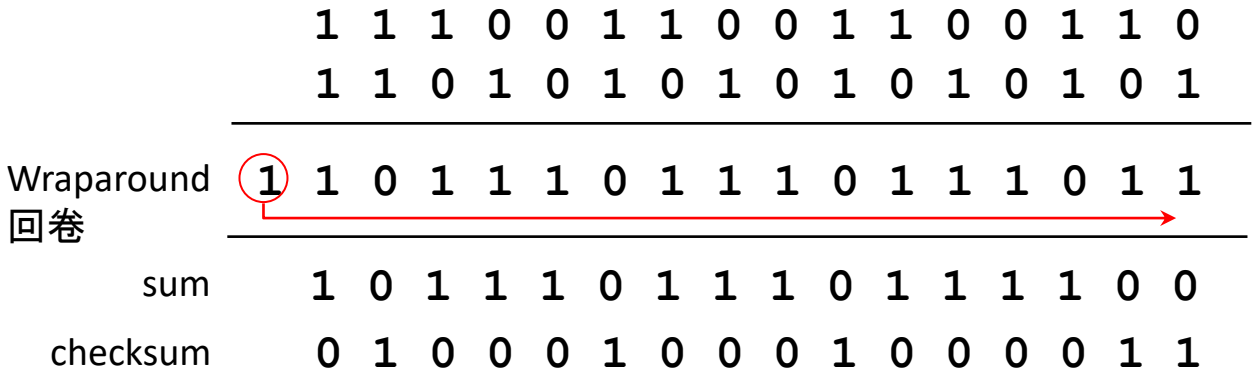
3.3 无连接传输层协议UDP

- 必要性：有些应用对实时性比较在乎，对可靠性要求不高
- 报文格式
  - 校验和计算（差错控制）：16bit二进制求和，进位回滚，反码

1、UDP和TCP使用的反码来计算他们的校验和。假设你有下面3个8bit字节:01010011,01100110,01110100。这8bit字节和的反码(即8bit的校验和)是11010001 。(紧凑格式:即不要有空格)

Internet checksum: an example

example: add two 16-bit integers

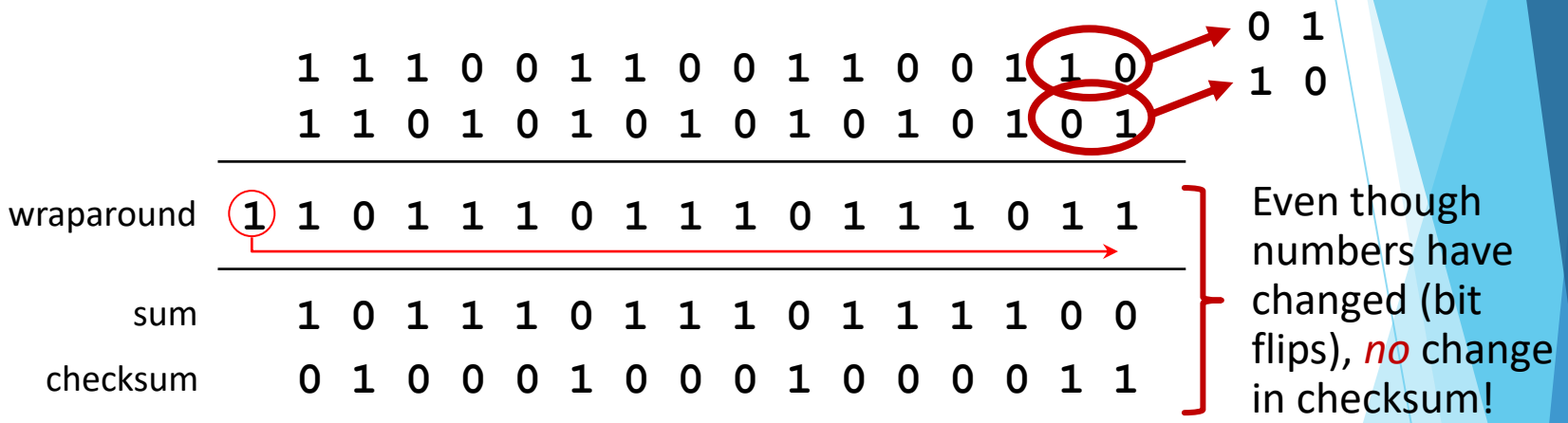


Note: when adding numbers, a carryout from the most significant bit needs to be added to the result(当数字相加时，在最高位的进位要回卷，再加到结果上)

* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Internet checksum: weak protection!

example: add two 16-bit integers



Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Secure remote terminal access	SSH	TCP
Web	HTTP, HTTP/3	TCP (for HTTP), UDP (for HTTP/3)
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	DASH	TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Name translation	DNS	Typically UDP

第三章 运输层

3.4 可靠数据传输原理

Mechanism	Use, Comments
Checksum（校验和）	用于检测在packet中的比特错误。
Timer（定时器）	用于超时/重传一个packet，可能该packet（或它的ACK）在信道中丢失了。当过早超时，或回包丢失时，都可能触发超时事件，所以接收方可能收到packet的冗余副本。
Sequence number（序列号）	用于对packet按顺序编号。编号可以用于检测packet的丢失或冗余
Acknowledgment（ACK）	接收方给发送方的正确反馈。确认报文通常携带被确认packet或多个packet的序号。确认可以逐个也可以累加。
Negative acknowledgment（NAK）	接收方给发送方的反向反馈。通常携带未被正确接收的分组的序号。
Window, pipelining	发送方允许一次发送多个未确认的packet，能发送的最大packet数量取决于窗口长度，窗口长度根据接收方接收和缓存报文的能力、网络中的拥塞程度或结合两者情况进行设置。

第三章 运输层

3.5 有连接传输层协议TCP

- TCP服务特性
  - 点到点服务，可靠、保序的字节流服务，管道服务（在未经确认的情况下一次能够传输多段数据），全双工通信，面向连接，流控制

- 报文格式
  - 序号：连接建立时协商好的双方的起始序号；每个TCP报文中的序号是首字节在字节流的偏移量
  - 确认：是对顺序收到的最后一个字节+1。
  - RST、SYN、FIN：拥塞控制
  - 接收窗口：流量控制

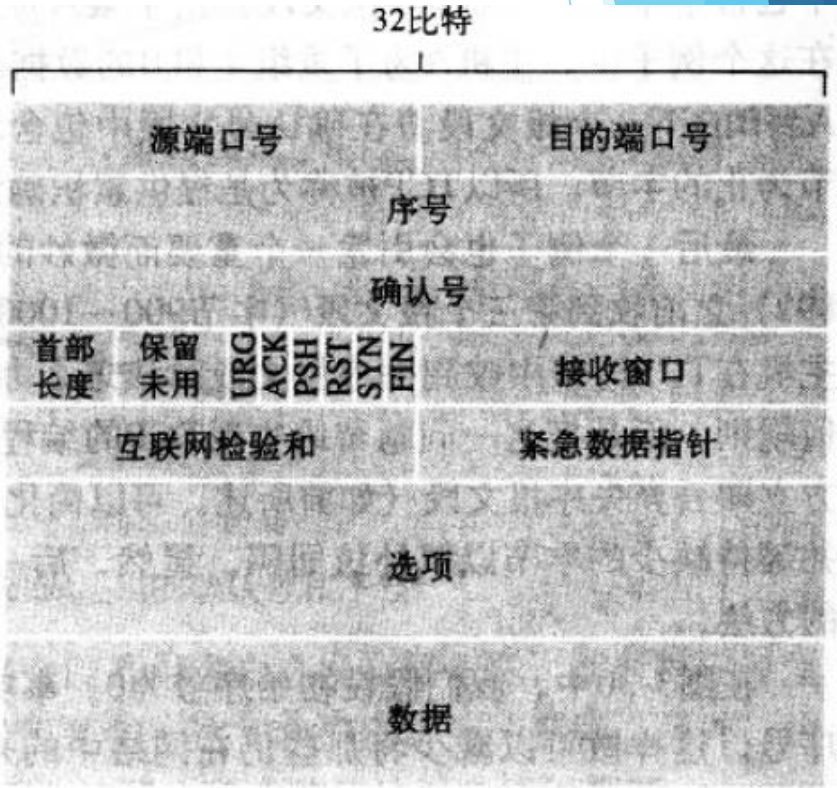
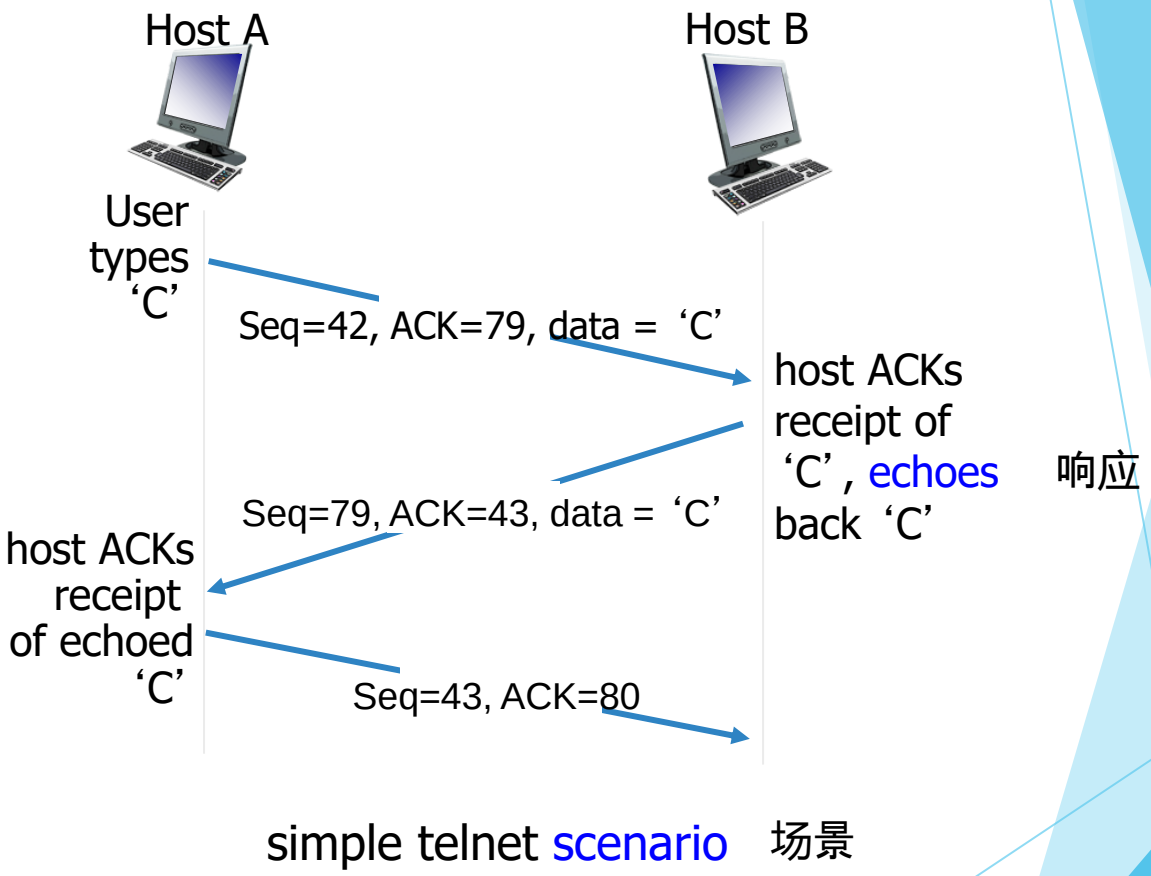


图3-29 TCP报文段结构

第三章 运输层

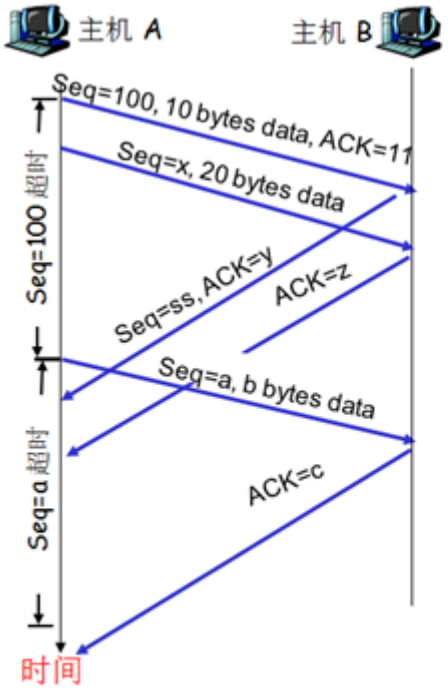
3.5 有连接传输层协议TCP

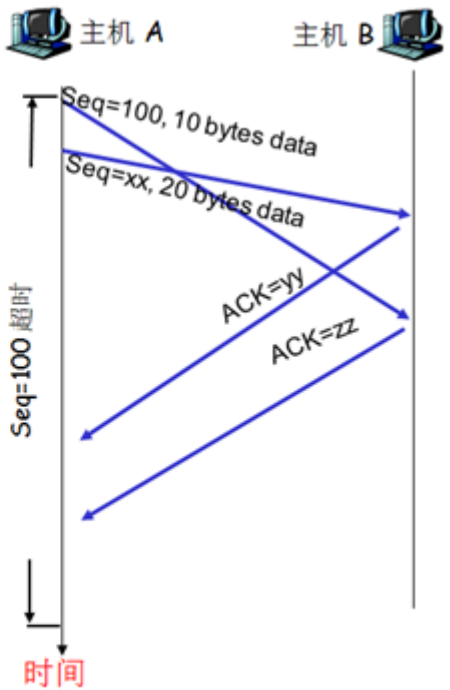


simple telnet scenario 场景

第三章 运输层

3.5 有连接传输层协议TCP





运输层 72

1、填写其中变量的值：x=( ), y=( ), z=( ); a=( ), b=( ), c=( ), ss=( ); xx=( ), yy=( ), zz=( )

第三章 运输层

3.5 有连接传输层协议TCP

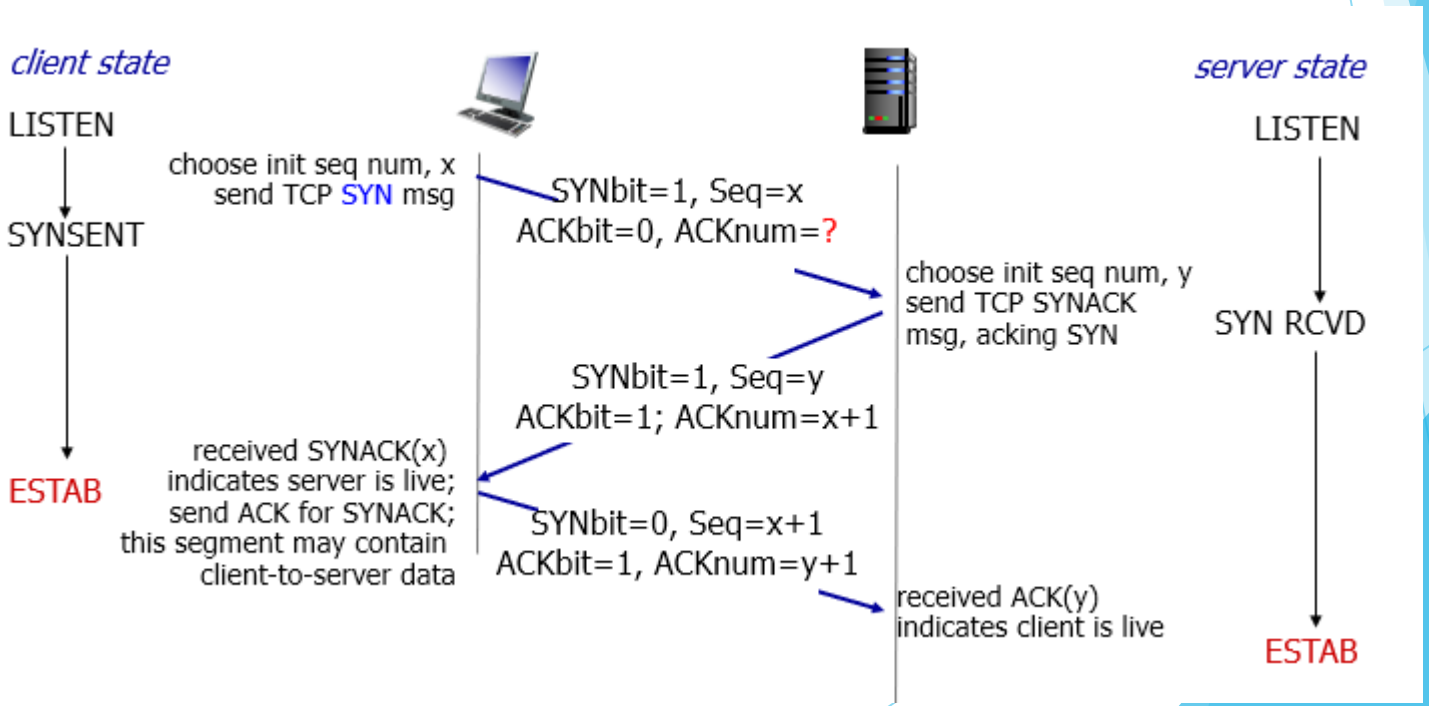
- RTT时间估计和重发超时时间估计
- TCP可靠数据传输
  - 累积确认
  - 只重传最早的未确认段
  - 快速重传：在没有超时的情况下，收到对方对于某一个段的重复三次（一共4个）ACK
- 流量控制
  - 目的：防止淹没接收方
  - 手段：将接收窗口大小捎带给发送端

1、TCP流控中,当接收方的接收窗口为0时,发送方继续发送__1__个字节数据的报文段。这些报文段将会被接收方确认。最终接收方缓存开始清空,并且确认报文中将包含一个非0的rwnd。

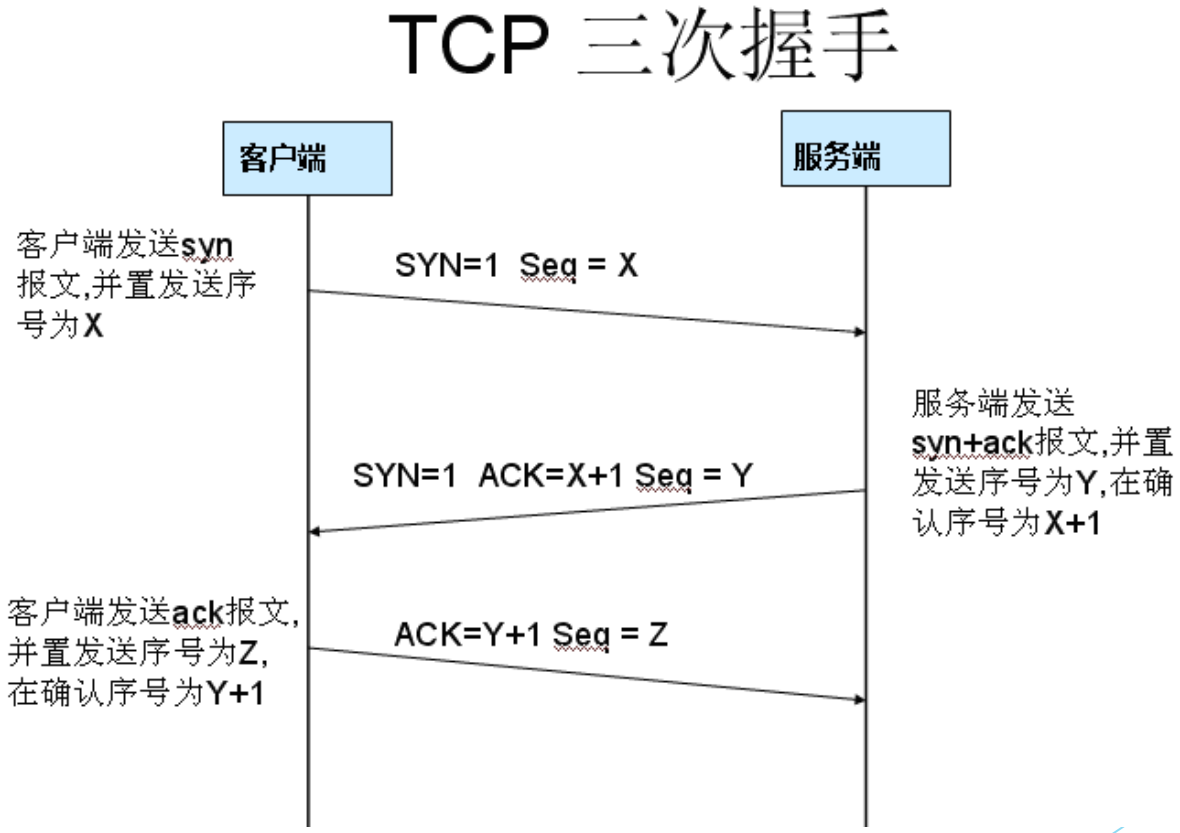
第三章 运输层

3.5 有连接传输层协议TCP

- 连接建立
  - 3次握手，对双方选择的初始序号给予确认，准备好缓冲区。
  - 第1次握手：SYN=1，ACK=0，发起端序号
  - 第2次：SYN=1，ACK=1，接收端序号
  - 第3次：SYN=0，ACK=1



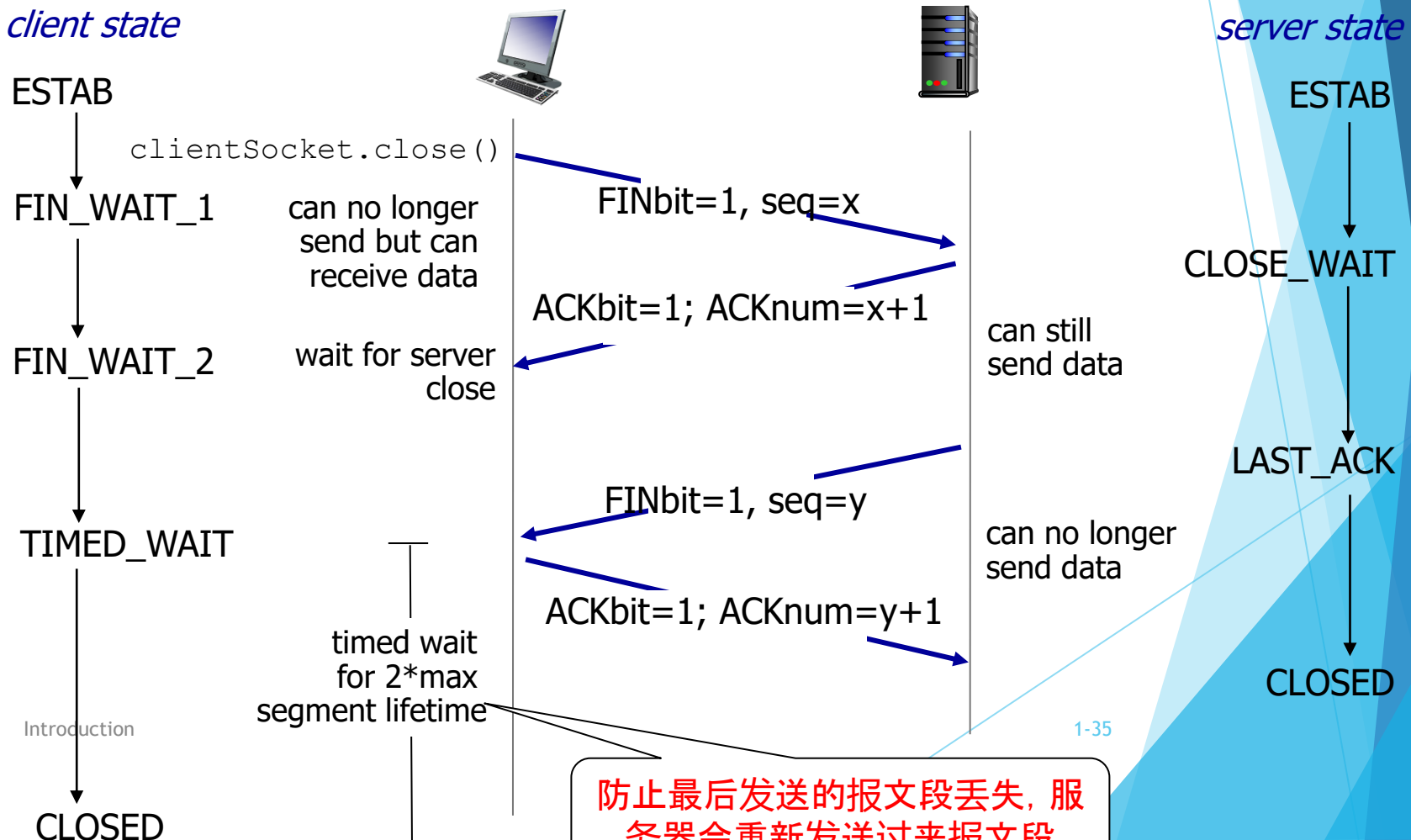
TCP的3次握手


TCP 三次握手
客户端
服务端
客户端发送syn报文,并置发送序号为X
SYN=1 Seq = X
服务端发送syn+ack报文,并置发送序号为Y,在确认序号为X+1
SYN=1 ACK=X+1 Seq = Y
客户端发送ack报文,并置发送序号为Z,在确认序号为Y+1
ACK=Y+1 Seq = Z

第三章 运输层

3.5 有连接传输层协议TCP

- 连接拆除（四次挥手）
  - 双方分别拆除自己的连接，对称，使用FIN字段



第三章 运输层

3.6 拥塞控制

- TCP使用端到端的拥塞控制
- TCP拥塞控制原理
  - 检测拥塞：超时（拥塞），三个冗余ACK（轻微拥塞）
  - 拥塞控制机制：AIMD　慢启动（连接建立时拥塞窗口值每个RTT增加一倍）　拥塞避免（线性增加拥塞窗口）
- TCP拥塞控制两种算法
  - Tahoe：超时和三个冗余ACK处理方式一样
  - Reno：超时和三个冗余ACK处理方式不一样

1、TCP拥塞控制中的AIMD,即“加法增大”(加性增AI)和“乘法减小”(乘性减MD)的含义是(A).(B)

•A、“加法增大”是指TCP执行拥塞避免算法后,在收到对所有报文段的确认后(即经过一个往返时间)，就把拥塞窗口 cwnd增加一个 MSS 大小,使拥塞窗口缓慢增大,以防止网络过早出现拥塞。

•B、“乘法减小”是指只要出现一次超时或重复确认(即出现一次网络拥塞)，就把慢启动阈值 ssthresh 设置为当前的拥塞窗口值乘以 0.5，并快速降低拥塞窗口而快速降低发送数率,避免网络一直拥塞;

第三章 运输层

3.6 拥塞控制

- TCP使用端到端的拥塞控制
- TCP拥塞控制原理
  - 检测拥塞：超时（拥塞），三个冗余ACK（轻微拥塞）
  - 拥塞控制机制：AIMD　慢启动（连接建立时拥塞窗口值每个RTT增加一倍）　拥塞避免（线性增加拥塞窗口）
- TCP拥塞控制两种算法
  - Tahoe：超时和三个冗余ACK处理方式一样
  - Reno：超时和三个冗余ACK处理方式不一样

TCP Tahoe：慢启动（slow start）、拥塞避免（congestion avoidance）、快速重传（fast retransmit）

超时和三个冗余ACK：cwnd降为1MSS，慢启动阈值降为原来的cwnd的一半，进入SS阶段，然后每个RTT后倍增，直到慢启动阈值，从而进入CA阶段

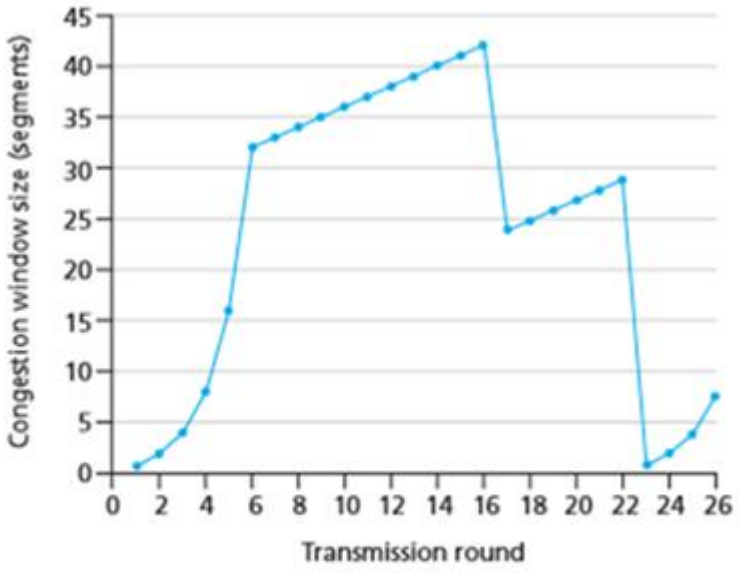
TCP reno：多了一个快速恢复（fast recovery）

1、超时：和Tahoe超时时处理方式一致

2、三个冗余ACK：cwnd值降为原来的一半，直接进入CA阶段

第三章 运输层

3.6 拥塞控制



gure 3.58 ♦ TCP window size as a function of time

1.TCP slow start(慢启动)运行时的时间间隔是：[1, 6] [23,26]

2. TCP congestion Avoidance(拥塞避免)运行时的时间间隔是：[6, 16] [17, 22]

3.在第16个传输回合后，报文段的丢失是根据3个冗余ACK还是根据timeout检测出来的？（3个冗余ACK ）

4.在第22个传输回合后，报文段的丢失是根据3个冗余ACK还是根据timeout检测出来的？（ timeout ）

5.在第1个传输回合后，ssthresh的初始值设置为多少？（32）

6.在第18个传输回合后，ssthresh的初始值设置为多少？（21）

7.在第24个传输回合后，ssthresh的初始值设置为多少？（ 14.5 ）

8.在哪个传输回合内发送第70个报文段？（ 7 ）

9.假设在第26个传输回合后，通过收到3个冗余ACK检测出分组有失，拥塞的窗口长度与ssthresh的值应当是多少？（7, 4）

10.假定使用TCP Tahoe，并假定在第16个传输回合收到3个冗余ACK。在第19个传输回合，ssthresh与拥塞窗口长度是什么？（21, 4）

11.再次假定使用TCP Tahoe，在第22个传输回合有一个timeout。从第17-22个传输回合（包括），一共发送了多少分组？（ 52 ）

1、[判断题]考虑TCP的拥塞控制。当发送方定时器超时时,其ssthresh的值将被设置为原来值的一半。(×)

2、[判断题] 假定一条TCP连接中最后的SampleRTT是1s,那么该连接的TimeoutInterval的当前值定大于等于1s。(×)

3、[判断题] TCP套接字、UDP套接字都是由二元组(目的IP地址,目的端口号)标识的。(×)

4、[判断题]运输层协议的作用是: 在运行在不同主机上的应用进程之间提供逻辑通信;网络层协议的作用也是这样。(×)

5、[单选题]在我们的rdt协议中,为什么要引入序号?(A)
A、让接收方区分收到的是新分组、还是重传的分组
B、用于检测超时/重传一个分组
C、用于检测在一个传输分组中的比特错误
D、接收方用于告诉发送方一个分组或一组分组已被正确地接收到了、或者检测到接收的分组有损伤
E、用于提高带宽利用率、提高性能

6、[多选题]为何要有 UDP协议?(ABCD)
A、无连接创建(不会引入建立连接的时延)
B、简单:在发送方、接收方无连接状态
C、段首部小
D、无拥塞控制、无流量控制: UDP能够尽可能快地传输

7、[多选题] [多选题] 网络拥塞的代价有(ABCE)。
A、拥塞时时延增大
B、比额定的“吞吐量”做更多的工作 (重传)
C、对迟延的分组(而不是丢失),有不必要重传: 链路承载分组的多个拷贝
D、拥塞时RTT减小
E、当分组丢失时, 任何用于传输该分组的上游传输能力都被浪费!

8、[判断题] UDP能提供进程到进程的“数据交付”和“差错检查”,TCP也能。(√)

9、[判断题] 假设主机A通过一条TCP连接向主机B发送一个大文件。如这条连接的一个报文段序号为m。则后继报文段序号必为m+1。(×)

10、[多选题] TCP拥塞控制中,发送方通过( )感知网络拥塞。(AC)
A、超时
B、肯定确认(ACK)
C、3个重复ACK
D、检测到分组受损

11、[多选题] 关于TCP的流量控制与拥塞控制,说法正确的是(ABCD)
A、流量控制指在给定的发送端和接收端之间的点对点通信量的控制;发送方不能发送太多、太快的数据让接收方缓冲区溢出;
B、拥塞控制是指在通信子网间所做的保证能够承载用户提交的通信量的控制;拥塞主要表现是丢包 (路由器缓冲区溢出)、长时延 (路由器缓冲区中排队);
C、它们的相同点是都需要在发送端对发送速率做控制,其目的都是为了减少丢包率,提高链路传输效率;
D、它们的区别在于拥塞控制是一个全局性的过程,涉及到所有的主机、所有的路由器以及与降低网络性能有关的所有因素;而流量控制所要做的就是抑止发送端发送数据的速率以便接收端来得及接收
E、UDP也有流量控制和拥塞控制。

12、[多选题]关于TCP协议和UDP协议的说法正确的是(ABC)
A、TCP协议和UDP协议都是运输层的协议。
B、UDP 在传送数据之前不需要先建立连接。对方的运输层在收到 UDP 报文后,不需要给出任何确认。虽然 UDP 不提供可靠交付,但在某些情况下UDP 是一种最有效的工作方式。
C、TCP 则提供面向连接的服务。由于TCP要提供可靠的、面向连接的运输服务,因此不可避免地增加了许多的开销。这不仅使协议数据单元的首部增大很多,还要占用许多的处理机资源。
D、TCP和UDP都提供流量控制、拥塞控制。

13、[多选问答题] TCP协议的特点有(ABCDEF)
A、点到点:一个发送方, 一个接收方;连接状态不被中间的路由器所知;
B、可靠数据传输
C、全双工数据:同一连接上的双向数据流
D、面向连接:在进行数据交换前,初始化发送方与接收方状态,进行握手(交换控制信息)
E、流量控制:发送方不能淹没接收方
F、拥塞控制:抑止发送方速率来防止过分占用网络资源
G、无连接:在发送方和接收方之间无握手

第四章 网络层

4.1 简介

- 网络层主要服务和功能
  - 服务：向传输层提供主机到主机的段的传输服务
  - 功能-转发（又名交换），数据平面功能：从路由器的一个端口流入，从另一个端口流出
  - 功能-路由，控制平面功能，决定从源到目的的路径
  - 两个功能相互配合将数据报从源传送到目标
- 实现网络层功能两种方式
  - 传统方式：控制平面和数据平面集成在每个设备上；路由协议实体分布式地计算路由表；IP协议按照路由表进行转发
  - SDN方式：控制平面和数据平面分离；sdn控制器集中计算；下发流表实现控制平面功能；sdn分组交换机按照流表表项进行操作。
- 网络层服务的重要指标
  - 带宽、延迟/延迟差，丢包与否/丢包率
  - 网络层提供的是尽力而为的服务：丢包、乱序、不可靠

第四章 网络层

4.2 路由器结构

- 路由器功能
  - 路由协议：使用路由算法，生产转发表和路由表
  - 转发分组：使用转发表转发分组
- 结构
  - 输入端口当给定目标地址查找转发表时，采用最长地址前缀匹配的目标地址表项
  - 输出端口：调度策略（FIFO、优先级、RR、WFQ）
  - 交换结构：基于内存的，基于总线的，基于crossbar的
  - 路由处理器

第四章 网络层

4.3 IP协议

- IPv4格式
  - 各字段作用
  - 分片和重组
- IP编址
  - IP地址：主机或路由器和网络的接口的标识，IPv4地址长度32bit，由网络号部分和主机号部分组成
  - 子网：在一个子网内的设备之间的通信有两个特点(1)通信无需借助路由器(2)子网前缀一样（网络号一样）
  - 有类地址划分
  - 特殊IP地址
  - 子网掩码和CIDR
- NAT协议
- DHCP协议：上网主机自动获得IP、掩码、默认网关和local name server
- 路由聚集
- IPv6协议
  - 格式：IPv6地址长度128bit
  - 相较于IPv4变化
  - IPv4到IPv6的迁移 隧道

点分十进制和二进制表示的转换，一定掌握！

IP地址的10进制与2进制转换

- Q:IP地址的206.0.71.128的二进制等价形式是多少？

8-bit 二进制位的权值依次为:

	0	0	0	0	0	0	0	0
	128	64	32	16	8	4	2	1
206=	1	1	0	0	1	1	1	0

206-128 = 78 （右边第一位(最高位)为1）

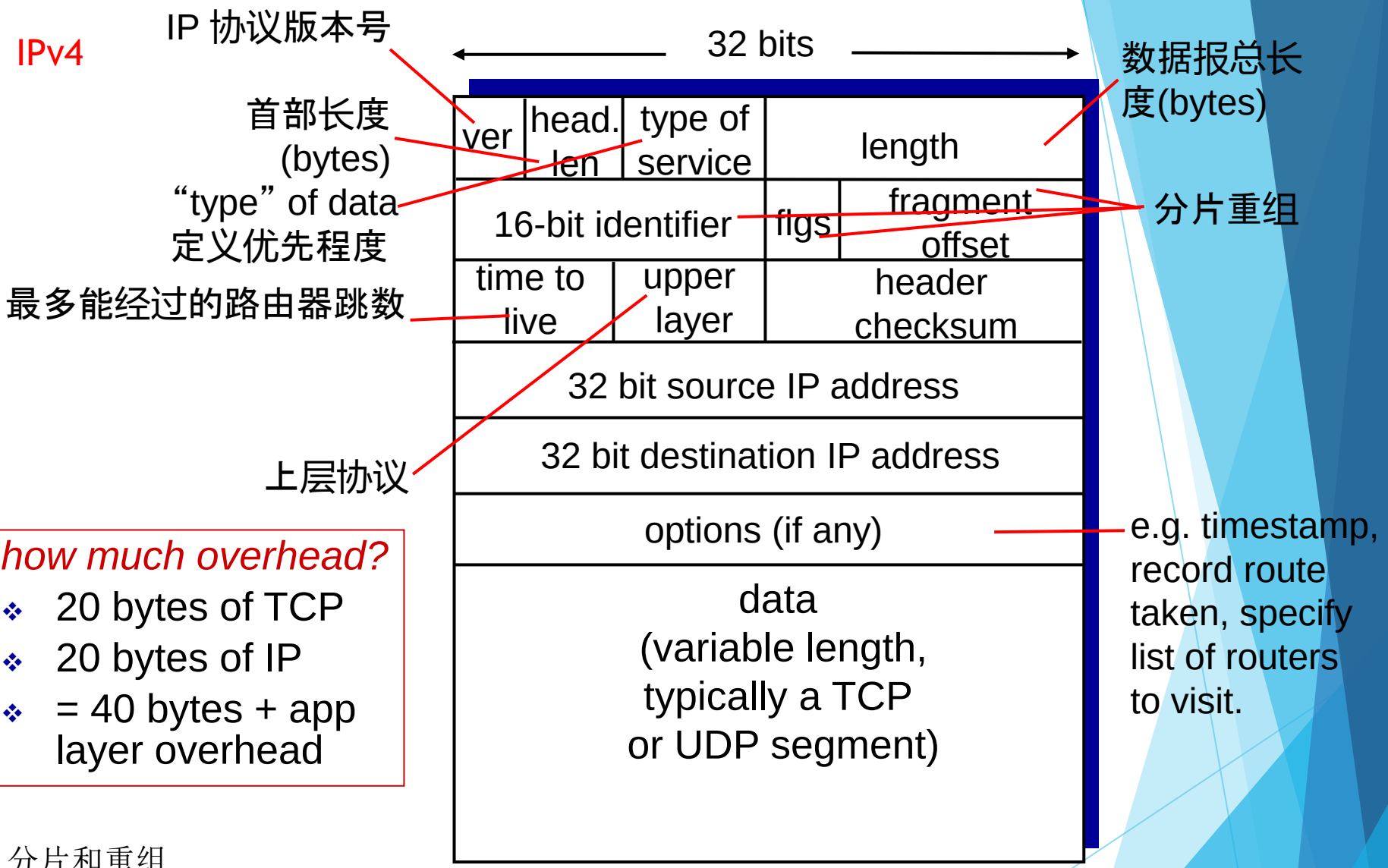
78- 64 = 14 （右边第二位为1）

14 - 32 不够减(右边第三位为0)

...

(或者对简单的14, 14 = 8 + 4 + 2 + 0)

IPv4



how much overhead?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

分片和重组

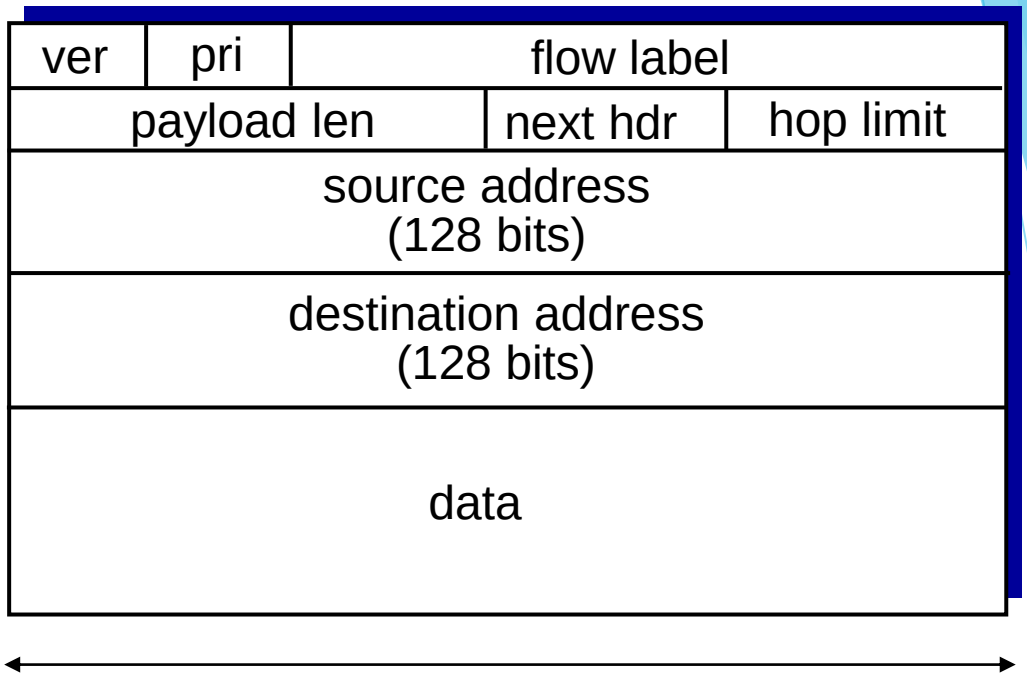
Identifier：同一个ID表示同一个分组，

flag标志位：如果是1，并非最后一片，如果为0，表示最后一片

Offset偏移量：当前数据报的数据部分第一个字节在原数据中的位置，值以1当8。

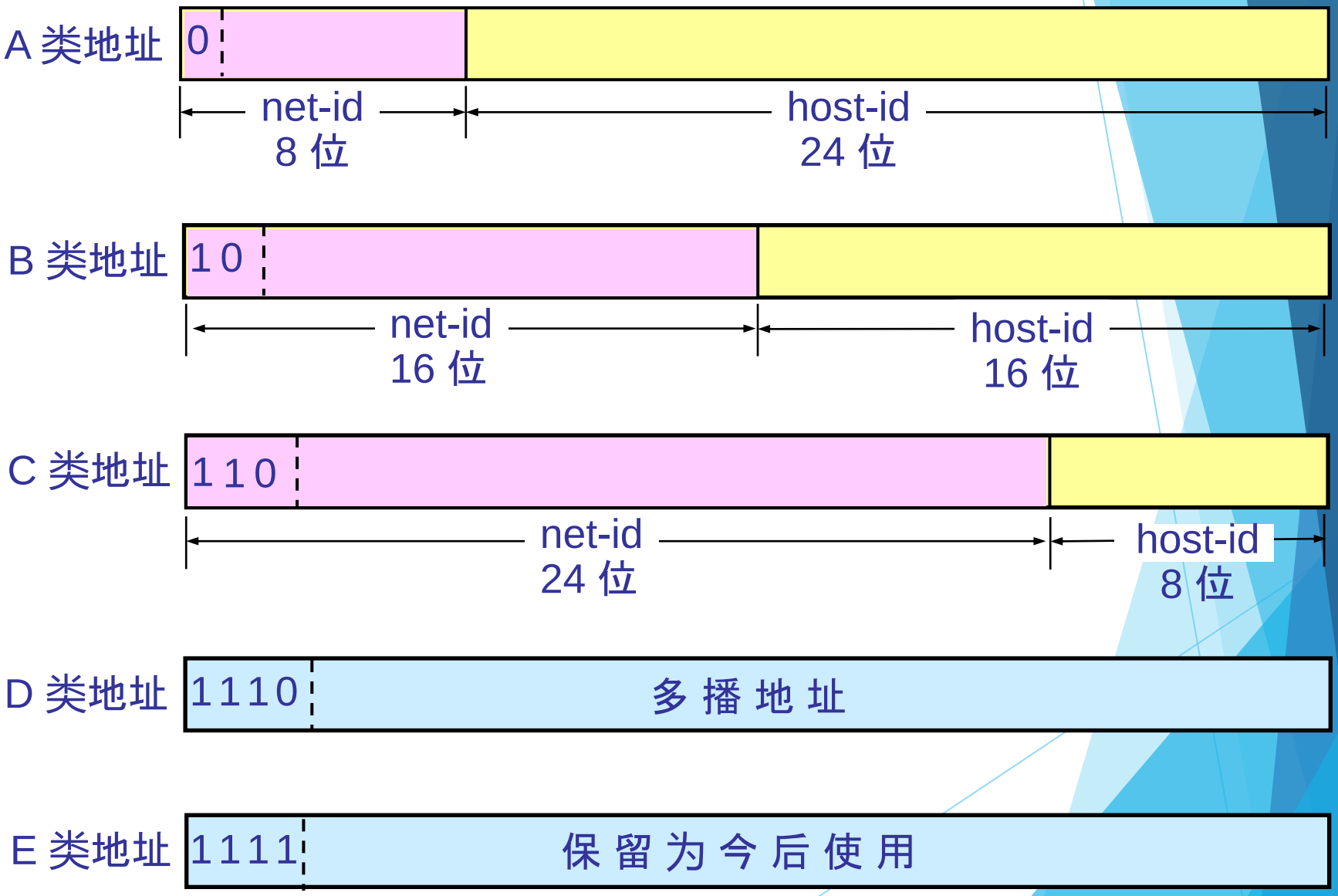
IPv4头部一般20字节

IPv6



pri：priority = IPv4中的type of service，优先级
flow label：流标签，同一个IP发出来的同一个会话的数据可以标记位同一个流，让网络为其预分配资源。
hop limit： = IPv4的ttl
next header = IPv4的upper layer，表示该数据报的上层协议，在IPv6中，还可以标识出载荷部分的选项
payload len = 数据长度
IPv6去除：checksum， 头部的选项字段， 不做分片重组
IPv6头部定长40字节！

IP 地址的分类


A 类地址
0
net-id
8 位
host-id
24 位
B 类地址
10
net-id
16 位
host-id
16 位
C 类地址
110
net-id
24 位
host-id
8 位
D 类地址
1110
多播地址
E 类地址
1111
保留为今后使用

IP 地址的分类

IP 地址的指派范围

网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中最大主机数
A	126 ($2^7 - 2$)	1	126	16777214
B	16383 ($2^{14} - 1$)	128.1	191.255	65534
C	2097151 ($2^{21} - 1$)	192.0.1	223.255.255	254

特殊IP地址

网络号	主机号	源地址使用	目的地址使用	代表的意思
0	0	可以	不可	在本网络上的本主机（见 DHCP 协议）
0	host-id	可以	不可	在本网络上的某台主机 host-id
全 1	全 1	不可	可以	只在本网络上进行广播（各路由器均不转发）
net-id	全 1	不可	可以	对 net-id 上的所有主机进行广播
127	非全 0 或全 1 的任何数	可以	可以	用于本地软件环回测试

私有地址

Class A 10.0.0.0-10.255.255.255 MASK 255.0.0.0;

Class B 172.16.0.0-172.31.255.255 MASK 255.255.0.0

Class C 192.168.0.0-192.168.255.255 MASK 255.255.255.0

IP addressing: CIDR

无类域间路由

CIDR: Classless InterDomain Routing

- 网络号可以为任意长度
- 地址格式: a.b.c.d/x, x 是地址中网络号部分的位数

11001000 00010111 00010000 00000000

200.23.16.0/23

子网掩码: 11111111 11111111 11111110 00000000

子网掩码

- 通过子网掩码可以把32位IP地址划分为两部分：网络号和主机号。
  - 老式写法：
    - IP：206.0.68.0，子网掩码:255.255.252.0
  - CIDR表示法：206.0.68.0/22
  - 1: bit位置表示子网部分
  - 0:bit位置表示主机部分

两种写法都需要掌握！

- 子网掩码与IP地址逻辑与后获得网络号，路由器按最长匹配原则决定转发端口：

  11001110 00000000 01000100 00000000

  11111111 11111111 11111100 00000000

  - 206.0.68.0/22的网络号是206.0.68.0
  - 那206.0.69.0/22的网络号是多少？

Subnets

应用二：某A类网络20. 0. 0. 0的子网掩码为255. 224. 0. 0，请确定可以划分的子网个数，写出每个子网的子网号。

解答：A类网络的默认子网掩码为255.0.0.0，根据题目，第二个字节的子网掩码为224，即11100000，可知，该A类网络用第二个字节的3个比特进行了子网划分。因此划分的子网数为$2^3=8$个。

8个子网的子网号分别为：

20.000 00000.0.0 即 20.0.0.0
20.001 00000.0.0 即 20.32.0.0
20.010 00000.0.0 即 20.64.0.0
20.011 00000.0.0 即 20.96.0.0
20.100 00000.0.0 即 20.128.0.0
20.101 00000.0.0 即 20.160.0.0
20.110 00000.0.0 即 20.192.0.0
20.111 00000.0.0 即 20.224.0.0

Subnets

应用三：将某C 网200. 161. 30. 0划分成4个子网，请计算出每个子网的有效的主机IP地址范围和对应的子网掩码。

解答： C 网200.161.30.0的默认子网掩码为255.255.255.0，即前三个字节200.163.30为网络号。
子网划分将从第四个字节的第一个比特开始。
现需要划分4个子网，即需要 $\lceil \log_2 4 \rceil = 2$个比特位，因此子网掩码为：
255.255.255.11000000，即255.255.255.192

子网1的网络地址:200.161.30.00000000，即200.161.30.0
子网2的网络地址:200.161.30.01000000，即200.161.30.64
子网3的网络地址:200.161.30.10000000，即200.161.30.128
子网4的网络地址:200.161.30.11000000，即200.161.30.192

所以，每个子网上的有效主机IP地址范围分别为（排除了全0和全1的主机地址）：
子网1 ： 200.161.30.00 000001~ 200.161.30.00 111110 ，即200.161.30.1 ~200.161.30.62
子网2 ： 200.161.30.01 000001~ 200.161.30.01 111110 ，即200.161.30.65 ~200.161.30.126
子网3 ： 200.161.30.10 000001~ 200.161.30.10 111110 ，即200.161.30.129 ~200.161.30.190
子网4 ： 200.161.30.11 000001~ 200.161.30.11 111110 ，即200.161.30.193 ~200.161.30.254

Subnets

应用四：某公司申请到的网络地址为192. 3. 2. 0，现要划分5个子公司，最大的一个子公司有28台计算机，每个子公司在一个子网中，则

(1) 子网掩码应为多少？

(2) 5个子公司的网络地址分别是什么？

解答： 网络地址为192.3.2.0，为C类地址，所以划分子网从第四个字节开始。

需要划分5个子网，应该需要 $\lceil \log_2 5 \rceil = 3$ 个比特。

第四个字节共8个比特，主机号占8-3=5位，因此每个子网可挂接2^5-2=30台主机。

根据题意，30>28，可以满足子公司的需求。

(1) 划分子网的子网掩码前三个字节为默认子网掩码，第四个字节的前三个比特为1，后五个比特为0，因此，子网掩码为255.255.255.11100000，即255.255.255.224。

(2) 可以划分2^3=8个子网，每个子网的网络地址分别如下：

192.3.2.000 00000 即 192.3.2.0
192.3.2.001 00000 即 192.3.2.32
192.3.2.010 00000 即 192.3.2.64
192.3.2.011 00000 即 192.3.2.96
192.3.2.100 00000 即 192.3.2.128
192.3.2.101 00000 即 192.3.2.160
192.3.2.110 00000 即 192.3.2.192
192.3.2.111 00000 即 192.3.2.224

Subnets

应用五：有一个网络号为128.119.40.128/26的一个子网。假定要把该子网再划分为4个子网，每个子网具有相同数量的IP地址。请写出这4个子网的前缀（形式a.b.c.d/x）。

解答：划为四个子网：4=2^2，需要增加2bit来作为子网地址：26+2=28，即需要128.119.40.128中的第四部分128（128=1000 0000）的最高4位作为网络地址的一部分（28位掩码）

1000 0000=128

1001 0000=144

1010 0000=160

1011 0000=176

故：128.119.40.128/28　　128.119.40.144/28

128.119.40.160/28　　128.119.40.176/28

Subnets

应用六：已知IP地址178.36.17.9/23,试根据二进制相与的方法求出其网络地址。

解答：

178.36.17.9/23的二进制表示10110010 00100100 00010001 00001001

子网掩码的二进制表示11111111 11111111 11111110 00000000

网络地址为IP地址与子网掩码相与，

结果为： 10110010 00100100 00010000 00000000

得出网络地址为 178.36.16.0

1. 一网络的现在掩码为255.255.255.248,问该网络能够连接( )个主机?

答：248=11111000 2^3=8，注意去除全0和全1地址，所以答案是6个主机
也可以用255-248+1=8个，去除全0和全1，也是6个主机（接口）

2.考虑向具有572B的MTU的一条链路发送一个1800B的数据报。假定初始数据报标有标识号311。（IPv4数据报格式中：“数据报长度”指的是首部+数据，以Byte计算）
将会生成（ 4）片
在生成相关分片的数据报中，第一片的各个字段中的值（数据报长度、标识、标志、偏移）是多少？（ 572， 311， 1，0)
在生成相关分片的数据报中，最后一片的各个字段中的值（数据报长度、标识、标志、偏移）是多少？（144，311，0，207 ）

3.考虑某路由器有如下的转发表：
Destination Network（目标网络）---- Outgoing Link Interface（出链路接口）
196.80.0.0/12 ----------1
196.96.0.0/12 ----------2
64.0.0.0/2 ----------3
Others ----------4

当该路由器收到目的IP地址为96.94.19.135的数据报，它将向接口（3 ）转发。
当该路由器收到目的IP地址为196.100.100.100的数据报，它将向接口（ 2 ）转发。

3.考虑某路由器有如下的转发表：

Destination Network（目标网络）---- Outgoing Link Interface（出链路接口）

196.80.0.0/12 ----------1

196.96.0.0/12 ----------2

64.0.0.0/2 ----------3

Others ----------4

(1)当该路由器收到目的IP地址为96.94.19.135的数据报，它将向接口（3）转发。

(2)当该路由器收到目的IP地址为196.100.100.100的数据报，它将向接口（2）转发。

(3)当该路由器收到目的IP地址为196.94.32.128的数据报，它将向接口（1）转发。

(4)当该路由器收到目的IP地址为197.95.32.128的数据报，它将向接口（4）转发。

4.考虑使用8比特主机地址的数据报网络。假定一台路由器使用最长前缀匹配并具有下列转发表：

前缀匹配 ---------- 接口

1 ----------1

11 ----------2

111---------- 3

其他 ----------0

前缀匹配	接口	地址范围	范围内的地址个数
111	3	111 00000~111 11111	32
11	2	110 00000~110 11111	32 （111开始的被接口2优先匹配掉了---最长前缀匹配规则）
1	1	10 000000~10 111111	64 （11开始的被接口2、3优先匹配掉了）
其他	0	00000000~0 1111111	128

注意问的是范围内的地址个数和能分配给主机的地址个数的区别！！

全0的作为网络地址使用，全1的作为广播地址，这两个地址不能分给主机。

5.考虑具有前缀128.129.80.128/26的一个子网。
(1)能被分配给该网络的主机IP地址（形式为xxx.xxx.xxx.xxx）的范围从小到大是：从（ ）到（ ），该范围内的有效IP地址个数是（ ）。
(2)假定要把该子网再划为生成4个子网，每个子网具有相同数量的IP地址。这4个子网（形式a.b.c.d/x）的前缀从小到大分别是（ ）、（ ）、（ ）和（ ）？

答：26位掩码：需要看128.129.80.128中的第四部分128的最高两位（128=10 000000）==》6位主机地址范围2^6-全0的-全1的=64-1-1=62
最小128.129.80.10 000001=128.129.80.129
最大128.129.80.10 111110=128.129.80.190
划为四个子网：需要2比特来继续区分网络：26+2=28,
即128.129.80.128中的第四部分128的最高4位作为网络地址的一部分（即新的4个子网是28位掩码）。
第四部分（128=1000 0000）要做新的变化（拿高位10后的2bits来区分4个子网），即：
1000 0000=128;
1001 0000=144;
1010 0000=160;
1011 0000=176
故新的4个子网如下：
128.129.80.128/28;
128.129.80.144/28;
128.129.80.160/28;
128.129.80.176/28

要求能写出划分子网的过程

[单选题] 因特网的应用层的分组(packet)名字是( );传输层的分组名字是( );网络层的分组名字是( );数据链路层的分组名字是( )

A、报文段(segment) 报文(message) 数据报(datagram) 帧(frame)

B、报文段(segment) 报文(message) 帧(frame)数据报(datagram)

C、报文(message) 报文段(segment) 帧(frame)数据报(datagram)

D、报文(message) 报文段(segment) 数据报(datagram) 帧(frame)

[判断题] 每个自治系统(AS)使用相同的AS内部路由选择算法是有必要的。 √

1、某路由器的转发表如左：当该路由器收到目的IP地址为右表第一列的数据报后， 它将数据报向对应的接口转发。请填写对应的转发接口在下表的第二列。（注：第一行为示例）
[填空1] [填空2] [填空3] [填空4] [填空5]

目标网络	出链路接口
10.13.4.0/23	1
10.13.0.0/16	2
10.13.5.128/25	3
其他	4

收到数据报的目的IP地址	转发接口
10.13.5.130	3
10.14.0.1	4
10.13.0.1	2
10.13.5.1	1
10.13.5.193	3
10.13.6.1	2

2、把网络117.15.32.0/22划分为117.15.32.0/27，则得到的子网是32个？每个子网中可用的主机地址是30个？

3、[单选]如果一个子网内的默认网关地址是172.30.10.34/28，则下列地址中能作为主机的有效地址的是 C
A.172.30.10.53 B. 172.30.10.47 C. 172.30.10.40 D. 172.30.10.32

4、现在考虑将IP 地址空间 192.168.80.0/25平均给2个子网，其中已为子网1的部分主机和路由器分配IP地址范围为192.168.80.1~192.168.80.20，已为子网2的部分主机和路由器分配IP地址范围为192.168.80.66~192.168.80.113。
则：写出子网1的广播地址是 192.168.80.63，子网2的前缀是 192.168.80.64/26（形式a.b.c.d/x)
若每个主机仅分配一个IP地址，那么子网2还能分配的主机数量是 14

第四章 网络层

4.4 通用转发和SDN

- SDN控制平面和数据平面分离的优点
  - 集中在控制器上实现控制逻辑，网络可编程，看i恶意实现各种复杂的网络功能，新功能一次部署、持续升级，方便管理
  - 形成开放生态（控制器、分组交换机、网络应用，在一个开放的框架下协助）
  - SDN分组交换机按照计算出的流表进行分组转发、通用、便于升级
- IP编址
  - 模式匹配+动作（转发、组播、泛洪修改字段、阻塞）
  - 对到来分组按照各级字段匹配流表，按照相应的行动操作分组
  - 按照优先权进行判断，之后统计基数
- 控制平面

4.5 ICMP协议

- 作用：包括报告错误、echo请求和响应
- 报文类型

第四章 网络层

4.6 路由选择算法

- 根据收集到的路由信息（拓扑、链路代价等）计算出源到目标的较好路径（代价比较低的路径）
- 链路状态算法（LS）全局的路由选择算法
  - 每个节点收集邻居信息，生成LS，LS全网泛洪
  - 节点收集LS状态分组，形成网络拓扑
  - 按照最短路径算法算出到其他节点的最优路径
- 距离向量算法（DV）局部的路由选择算法
  - 每个节点维护到所有其他节点的下一跳地址和代价
  - 邻居节点之间定期交换DV
  - 按照Bellman-Ford不断迭代生成到所有目标的代价和相应的下一跳
- 层次路由，自治系统
  - 内部网关协议：RIP（DV）、OSPF（LS，AS内部支持分层路由，同时支持多种代价）
  - 边界网关协议BGP：DV
  - 内部网关协议重视效率、性能看，外部网关协议重视策略

第五章 数据链路层局域网

5.1 引论

- 链路层提供的服务　数据链路层负责从一个节点通过链路将（帧中的）数据报发送到相邻的物理节点
  - 封装成帧，链路存取控制（链路访问控制）
  - 在相邻节点间进行可靠数据传输
  - 流量控制
  - 检错和纠错
  - 全双工和半双工服务
- 链路层网络节点连接方式
  - 点对点：更适合广域网
  - 多点连接：比较适合局域网、联网方便，但需要解决MAC问题
  - 按照最短路径算法算出到其他节点的最优路径

5.2 检错和纠错

- 奇偶校验
- CRC（**循环冗余检测**）
  - 用于***错误检测***，原理
  - 生成多项式
  - 冗余位计算方法以及验证方法

第五章 数据链路层局域网

5.3 多路访问协议

- MAC协议的必要性
- MAC协议
  - 信道划分 channel partitioning：TDMA、FDMA、CDMA
  - 随机访问 random access：CSMA、CSMA/CD、 CSMA/CA
  - 轮转协议 taking turns
- CSMA/CD基本原理：
  - 1、先听后发，信道忙:延迟传送，信道闲:传送整个帧
  - 2、边听边发：发送同时进行冲突检测
  - 3、冲突停止：一旦检测到冲突就立即停止传输, 尽快重发。
  - 4、随机延迟后重发：二进制退避原则重发
  - 目的:缩短无效传送时间,提高信道的利用率。

第五章 数据链路层局域网

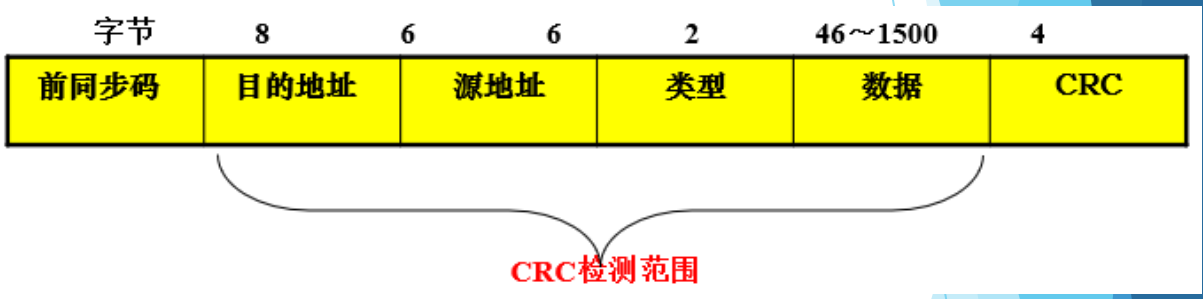
5.4 链路层编址

- MAC地址
  - 格式：48bit二进制，16进制表示，eg：1A-2F-BB-76-09-AD
  - 广播地址：48位全1 FF-FF-FF-FF-FF-FF
  - 分配
- MAC地址和IP地址的区别
  - 层次不同
  - MAC地址是平面的，用于标示一个物理网络的不同站点；IP地址是层次性的。
- ARP协议
  - 目的：物理网络范围内的IP地址到MAC地址的转换
  - 工作原理：广播查询，单播响应

第五章 数据链路层局域网

5.5 以太网

- 以太网使用IEEE802.3标准，具有链路层和相应的物理层
- 无线wlan使用IEEE802.11
- 网络拓扑结构：总线拓扑、星型拓扑、环形拓扑、网状拓扑、树形拓扑
- 以太网络的帧结构



- 向上提供服务的特点
  - 无连接
  - 不可靠
- 访问控制技术
  - 以太网使用CSMA/CD
  - Wlan使用CSMA/CA

第五章 数据链路层局域网

1. OSI/RM参考模型最底层是(物理层)

2.下面的哪句话最准确地说明了TCP/IP?(C)
A、它是一个单独的协议 B、它只代表两个协议 C、它是互联网协议的集合
D、所有网络协议的集合

3. CRC的作用是(B)。
A、封装成帧 B、差错检测 C、透明传输 D、地址转换

4. 对数据d = 0111000110101011进行1比特的偶校验,校验位的值是__1__。
解析：奇（odd）校验： 包括校验位后的整个数据中的1的个数为奇数；
偶（even）校验： 包括校验位后的整个数据中的1的个数为偶数；

第五章 数据链路层局域网

5.目前我们使用最广泛的LAN标准是基于什么协议的标准? (A)
A、802.3 B、802.4 C、802.5 D、802.11
题目解析:
IEEE802标准系列。
IEEE802委员会:美国电气和电子工程师协会在1980年2月成立的一个分委员会,专门制订局域网的相关标准
典型标准:
IEEE 802.3:CSMA/CD以太网。
IEEE 802.4:令牌总线网。
IEEE 802.5:令牌环形网。
IEEE 802.11:无线局域网。
IEEE 802.12:新型高速局域网(100Mb/s)